San Diego Mayor's Cyber Cup

Description and Procedures

30 November 2011

UCSD

NATIONAL DEFENSE INDUSTRIAL ASSOCIATION
NDIA
STRENGTH THROUGH INDUSTRY & TECHNOLOGY

SAIC
From Science to Solutions

TABLE OF CONTENTS

Competition Schedule 2
History of the Event 3
Mission and Objectives 4
Overview of Competition 4
Description of Rounds 5
Scoring Described 15
Other Items 16
Description of CyberNEXS 17
Profile of Blue System for Practice Round 18
Profile of Blue System for Qualification Round 18
Profile of Blue Systems for Finals 19

25 January 2010

Letter from the San Diego Chapter NDIA President

The San Diego defense industry recognizes the need for a work force grounded in the scientific and engineering disciplines, capable of supporting the high technology industrial base that has been essential to the nation's military and, accordingly, the local economy.

The failure of our education system to keep pace with the need to train this work force, as evidenced in data comparing our graduates with those of other nations, needs to be addressed by public policy, educators, and corporate America. Developing a response that will improve the ability of American students to compete for job s calling for skills in math science, and engineering will require a partnership of these stakeholders. As the voice of of the San Diego defense industry, the San Diego National Defense Industrial Association Chapter is committed to fostering this partnership and playing an active role in improving the performance of our local students in science, technology, engineering and mathematics (STEM). Additionally, the Chapter is committed to encouraging local students to pursue a career in the engineering and scientific fields.

The San Diego Mayor's Cyber Cup computer security competition provides one avenue for attracting and retaining young engineers and scientists. SAIC's CyberNEXS provides an environment in which students of all levels of knowledge can learn and practically apply their knowledge of computer network operations and their skills at portecting vital computer systems.. Through this competition, NDIA hopes to increase the level of excitement for learning technology in a stimulating, video game-like environment that provides immediate feedback.

NDIA sponsored a pilot cyber defense competition in 2008, which was highly successful and encouraged us to institutionalize this event. The University of California, San Diego (UCSD) and Science Applications International Corporation (SAIC) are the local "educators and corporate America" who have combined forces to conduct this second San Diego-based STEM initiative. UCSD will coordinate school participation and act as the independent judge to ensure the fairness of this competition. SAIC will conduct the competitions using their patent-pending trainer CyberNEXS cyber defense system which provides training, exercising, competitions and certification.

We are particularly pleased that the Mayor of San Diego, Jerry Sanders, has agreed to co-sponsor this event as the "San Diego Mayor's Cyber Cup". We believe this event will grow each year in participation and its importance in meeting the STEM challenge.

Kenneth Slaght
Rear Admiral, U.S. Navy (Ret.)
President
San Diego Chapter
National Defense Industrial Association

Competition Schedule

Tuesday, January 30 – Thursday, February 2: Practice Round (Anytime during window) - Remote

Friday, February 10 (4pm) – Saturday, February 11 (6pm): Qualification Round (Anytime during window) - Remote

Friday, February 24 (4pm) – Saturday, February 25 (6pm): Qualification Round (Anytime during window) - Remote

Saturday, March 10 (10am – 430pm): Finals Round, San Diego Supercomputer Center Auditorium at UCSD

Saturday, March 10 (5-7pm): Awards Banquet, UCSD Faculty Club

History of the Event

In the fall of 2007, the National Defense Industrial Association (NDIA) San Diego Chapter selected cyber security competitions as one of their key Science, Technological, Engineering and Mathematics (STEM) initiatives for 2007-2008. The University of California San Diego (UCDS) Physical Sciences Department and SAIC's Intelligence and Information Systems Business Unit teamed to deliver the NDIA Cyber Defense Competition. In the spring of 2008, five San Diego-based High Schools participated in this proof-of-concept competition. Each school met at the SAIC Campus Point facility, where SAIC provided baseline instruction on Windows Security in the morning, followed by pizza for lunch and then the competition in the afternoon. San Diego Mayor, Jerry Sanders, attended the final event. After the five individual training and exercising events, UCSD hosted a Banquet to announce the winners and present the awards; everyone expressed great interest in when the next competition of this kind could be conducted.

Last year, SAIC had developed a second generation competition system called the Cyber Network Exercise System (CyberNEXS), which provided a highly scalable training, exercising, competition and certification system. This technology and procedures had been tested and validated during the Air Force Association Cyber Patriot II National High School Cyber Defense competition series, which included several qualification rounds that were run via the Internet. The San Diego Mayor's Office agreed to institutionalize this important STEM outreach activity and, thus, the San Diego Mayor's Cyber Cup (SDMCC) was born. Three San-Diego high schools and one Orange County middle school competed in the inaugural SDMCC.

NDIA is sponsoring the competition as part of its STEM outreach program. ESET is again providing scholarships for the top teams. UCSD is coordinating the registration of teams. The San Diego Supercomputer Center has donated the use of their Auditorium for the Final Round competition. SAIC is providing the competition engine and the labor to conduct this three-phase program. All organizations are providing this support in-kind.

Mission and Objectives

Mission

To encourage and retain students in the degree and certification programs of Science, Technology, Engineering and Mathematics (STEM) disciplines.

Objectives

- Encourage students to learn about information assurance and computer security;
- Provide an educational venue in which students are able to apply the theory and practical skills they have learned;
- Foster a spirit of teamwork, ethical behavior, and effective communication both within and across teams;
- Create interest and awareness among participating schools and students; and,
- Encourage students to consider information assurance and computer security as a possible career path and/or as a possible course of study to pursue in higher education.

Overview of Competition

The San Diego Mayor's Cyber Cup invites all San Diego High Schools to participate in this three phase cyber defense competition series (discussed in detail below). The first two rounds will be using the distributed game mode, such that all San Diego High Schools can train and then compete simultaneously via the Internet. The eight winners of the qualification round will then participate in a head-to-head comprehensive centralized game, wherein all teams have individual CyberNEXS environments. This environment provides for 8-10 Blue (contestant) Targets, Red (Hacker) and White (Referee) Team resources and the scoring system (ScoreBot).

During the final competition, contestants will be scored on their ability to administer the following four essential skills:

1) maintenance of critical services;
2) removing vulnerabilities and hardening systems;
3) communicating status and resource requirements; and,
4) thwarting and removing hacker activities.

The finals will be conducted at UCSD Campus, with eight teams competing head-to-head in a very challenging environment complete with UNIX and Windows servers and workstations, as well as network and security devices. Each team will be individually scored on a minute-by-minute basis, such that at the end of the day, a winner is declared and then recognized at an Awards Banquet.

Description of Rounds

Practice Round

Overview

Practice Round – Distributed Game - Typically used during the initial rounds of a competition when there is a large number of people/teams competing. This round provides contestants with vulnerable targets (i.e. Windows and/or UNIX operating systems as VMware images) which are downloaded to the contestant's personal computer. At the beginning of the Practice Round, they are provided with the password that will unlock the Target contents. Once unlocked, the contestant will register their system via a GUI interface, which will confirm their successful registration. Once that registration is complete they can verify their individual score via a web page linked on their machine (ScoreBox). They will then begin to remove all vulnerabilities (harden) prior to end of the Practice Round. During that time, as their score improves, their ScoreBox will be automatically updated. The goal is to fix the most vulnerabilities, in the fastest time. This Practice Round also provides the opportunity to validate that their hardware and network configurations are suitable for the actual competition.

Rules

1) Student (Blue) Teams

1. Each team will consist of up to five (5) student members.
2. Each team may have one advisor present at the competition. The advisor may assist and/or advise the team during the Practice Round Only.
3. Each team will designate a Team Captain for the duration of the competition to act as the team liaison.
4. Contestants may use any computer and any tool, including the internet, during the conduct of the Practice Round.

2) Practice Systems

1. Each team will use their own computer and begin the competition with identically mis-configured VMware images(s)**.
2. Teams should not assume any competition system is properly functioning or secure; they should act as recently hired administrators who are now assuming responsibility for each of their systems.
3. All teams will be connected to the CyberNEXS scoring system, and will have near real-time feedback on their status of completion.
4. If a Team's system is not successfully registered with the CyberNEXS server, they will receive no score. Once registered, the Team will receive the score documented by the CyberNEXS server when the Team system was last connected.

3) System Requirements for Distributed Game Contestants

Hardware Requirements are as follows:

a. 1 Ghz Intel compatible processor (AMD processors have had issues with VMware and are not recommended);
b. 2 GB RAM;
c. 10 GB of free disk space;
d. Keyboard & Mouse;
e. 1024x768 or higher display;
f. (Optional) It is recommended to use a projector or large display to share the screen output with the rest of the team, but not required; and,
g. Network connection from computer(s) to Internet.

Software Requirements are as follows:

A. Operating System (Windows 2000 or newer, recent VMware supported Linux, or Macintosh 10.4.11 or later);
B. Web Browser;
C. SSH Client;
D. VPN Client; and,
E. VMware Player.

Internet Connectivity Requirements are as follows:

A. Minimum of 256kb uplink/downlink; and,
B. Network firewalls and/or Web Proxies should permit un-filtered TCP port 80 out-bound from your network from each of the computer(s) involved in the competition to the SAIC CyberNEXS server, cybernexs.saic.com.

NOTE: VMware image – Using virtualization technology, an entire operating system and resources can be captured as a file, and then replayed (using VMware Player) on Windows and UNIX operating systems. In other words, one can run a completely different computer system in a container, within the host operating system, that is on the competitor's computer. **When playing the Game, make sure you are taking the appropriate action within the VMware image.

4) Practice Play

The Practice Round will include the following two events:

A) Initial Download–The students will go to the SAIC site: http://cybernexs.saic.com/. There, contestants will download two VMware images: "Practice Target" and "Qualification Target". There will also be a word document that provides instructions for unlocking and registering the VMware image with the CyberNEXS server. These downloads will be password protected. The Practice Target password will be provided during the download process; the Qualification Target password will be provided at the start of the exercise (STARTEX). These images are hundreds of megabytes in size; therefore, they should be downloaded at the earliest opportunity using the fastest connections available, verified against their published MD5 checksums, and then brought

to the computer that will be used for the competition. The Practice Round registration site will not be active until STARTEX.

B) Practice Round –The purpose of the Practice Round is to provide Teams with an opportunity to validate that their hardware and network configurations are suitable for the actual competition, as well as provide time to learn about VMware images and how to successfully score on them. By successfully registering, the students will know that they are ready to compete by viewing their individual web status page. Once registered, each Team is permitted to "play the game" and will receive their score via the Feedback page. This link will be available for two days only.

IMPORTANT!!! STEPS TO COMPLETE REGISTRATION - There are the steps that you need to accomplish in the specified order to successfully register your VMware image with CyberNEXS:

1. Download Utility Programs

a) Download and install VMware Player: http://www.vmware.com/products/player/
b) Download and install a ZIP program like 7-zip: http://www.7-zip.org/
c) Download an MD5 checksum utility: http://winmd5.com/

2. Download VMware Images and Instructions; Verify MD5 hash:
http://cybernexs.saic.com/Downloads

a) Download the Practice and Qualification Round Instructions
b) Download the Practice Round Image Zip File [NOTE: MD5 checksum will be listed at time of download, (an example of an MD5 checksum is: fb5bc4b8142d3010a8e7ed0bdef2d195)].
c) Download the Qualification Round Image Zip File [NOTE: MD5 checksum will be listed at time of download].
d) Verify the MD5 checksum(s) for both ZIP files, if the numbers don't match, then the down load is corrupt and must be re-downloaded,

3. Verify MD5, Unpack Images and Validate Internet Access

a) Un-pack the Practice Round Image Zip File using password provided at:
http://cybernexs.saic.com/Downloads
b) Start VMWare Player, and open the Practice Round Virtual Machine (VM)
c) Once the Practice Round VM, has opened, inside the VM window - open a web browser
d) Verify that your Practice Round VM can get to any internet site (www.google.com, www.cnn.com)
(If not then consult with your local IT department for steps to enable)

4. Registering for Game

a) Once the Practice Round VM boots, a registration page appears before Login. In this registration window select your school from the drop-down menu, enter your team nick name and system name**. IMPORTANT, the nick and system names can be anything you want, but all three must be completed and submitted before you can compete. All actions are not scored until you are successfully registered.**
b) Once the Practice Round VM is completely registered a "Get My Status" link will appear in the "C:\" path on the VM. Open this link by double clicking, to show your Status.

c) After 1 minute or less, the Web page should change and say "The exercise is not started yet" and will give you a status of vulnerabilities. As you remove vulnerabilities in the Practice VM that were pre-configured for the game, you should receive notification via this Web Status Page.

5. Play the Game

You are now done with registration process; proceed with getting comfortable with the game; your score will tell you how well you are removing vulnerabilities.

Qualification Round

Overview

Qualification Rounds –Distributed Game –This is similar to the Practice Round, with a winner declared at the end of exercise. The winner will be selected based on the highest score at the end of the exercise. If there are two or more identical scores, the earlier score is the winner.

Rules

1) Student (Blue) Teams

- **a)** Each team will consist of up to eight (8) student members.
- **b)** Each team may have one advisor present at the competition. The advisor may not assist nor advise the team during the actual competition.
- **c)** Each team will designate a Team Captain for the duration of the competition to act as the team liaison.
- **d)** Contestants may use any computer and any tool, including the internet, during the conduct of the competition.
- **e)** The judges' decisions on any subject will be final.

2) Competition Systems

- **a)** Each team will use their own computer and begin the competition with identically mis-configured VMware images(s)**.
- **b)** Teams should not assume any competition system is properly functioning or secure; they should act as recently hired administrators who are now assuming responsibility for each of their systems.
- **c)** All teams will be connected to the CyberNEXS scoring system, and will have near real-time feedback on their status of completion.
- **d)** If a Team's system is not successfully registered with the CyberNEXS server, they will receive no score. Once registered, the Team will receive the score documented by the CyberNEXS server when the Team system was last connected.

**NOTE: VMware image – Using virtualization technology, an entire operating system and resources can be captured as a file, and then replayed (using VMware Player) on Windows and UNIX operating systems. In other words, one can run a completely different computer system in a container, within the host operating system, that is on the competitor's computer.

3) Competition Play

This competition series will be conducted using Windows Operating System Targets only and will include the following Events:

a) Qualification Round s: The students should already have downloaded the Qualification Target. On competition day at 15 minutes prior to STARTEX, the teams will be provided the password for the Qualification Target. The password will be posted to the SAIC website listed above. Once received, the students should unlock the Qualification Target as they did during the Practice Round. This new image will need to be registered with the CyberNEXS server (ScoreBot). At STARTEX, the students should begin the competition and will have four hours in which to fully "harden" (remove all vulnerabilities) prior to the end of the exercise (ENDEX). During that time, they can access their individual web status page for a time-delayed view of the percentage of vulnerabilities fixed. SAIC will be monitoring all scores in the ScoreBot database.

4) Scoring

a) Winners that will proceed to the finals will be selected as those teams that achieve the highest score first. If there is a tie for score, then the team that achieved that score earliest will be one of the qualifiers. NDIA will announce the eight finalists within 24 hours, and their names will be listed on the SAIC site: http://cybernexs.saic.com/.

b) Scores will be maintained by the SAIC White Team in the CyberNEXS Data Center in San Diego, CA. During the competition, each contestant team may view their progress at their individual web page reporting the percentage of vulnerabilities fixed. No other team will know the degree of success of the other teams; only the top eight teams and their scores will be announced

1. System Requirements for Distributed Game Contestants

Hardware Requirements are as follows:

A. 1 Ghz Intel compatible processor (AMD processors have had issues with VMware and are not recommended);
B. 2 GB RAM;
C. 10 GB of free disk space;
D. Keyboard & Mouse;
E. 1024x768 or higher display;

F. (Optional) It is recommended to use a projector or large display to share the screen output with the rest of the team, but not required; and,
G. Network connection from computer(s) to Internet.

Software Requirements are as follows:

A. Operating System (Windows 2000 or newer, recent VMware supported Linux, or Macintosh 10.4.11 or later);
B. Web Browser;
C. SSH Client;
D. VPN Client; and,
E. VMware Player.

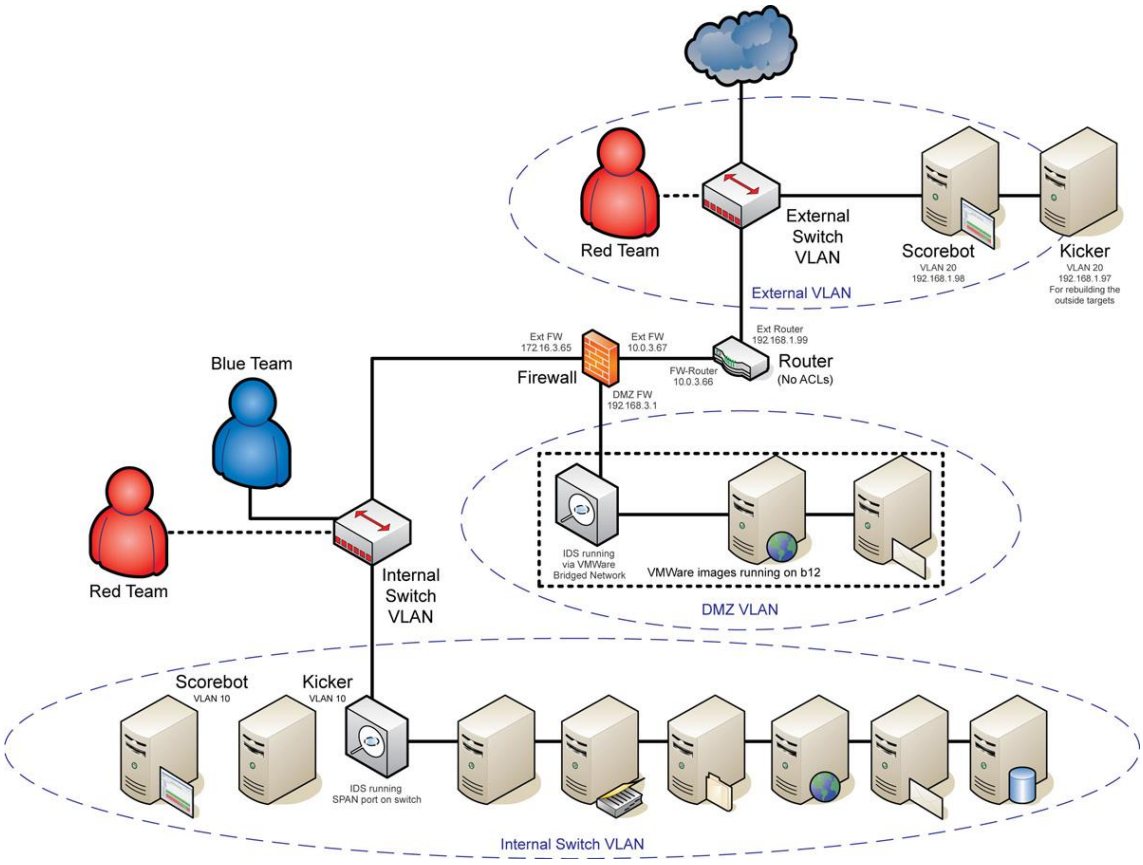
Internet Connectivity Requirements are as follows:

A. Minimum of 256kb uplink/downlink; and,
B. Network firewalls and/or Web Proxies should permit un-filtered TCP port 80 out-bound from your network from each of the computer(s) involved in the competition to the SAIC CyberNEXS server, cybernexs.saic.com.

Finals Round

Overview

Finals Round – Centralized Game – typically used when there are a few contestants, running a comprehensive exercise to test their ability to maintain critical services, harden systems, thwart attackers and communicate to report status and seek assistance. This final round of the Mayor's Cyber Cup will be conducted with eight final teams going head-to-head in the SAIC CyberNEXS centralized game. This game provides contestants with their own complete CyberNEXS environment, including Windows and UNIX operating systems, switches and router, firewalls and intrusion detection devices. At the beginning of the competition, the contestants will log into CyberNEXS, assume control of their "Blue" (exercise) systems, and begin to harden them as quickly as possible. Sometime later, the "Red" team (hackers) will begin to attack their systems. During all of this activity, contestants are expected to submit trouble tickets to request support (i.e. load patch, etc.) and to report status.



Finals Round Sample Architecture

Rules

1) **Student (Blue) Teams**
   - **a)** Each team will consist of up to eight (8) members. Each team member must be a full-time student of the high school they represent.
   - **b)** Each team may have one advisor present at the competition – this may be a faculty/staff member of the school or a unit sponsor. The advisor may not assist or advise the team during the competition.
   - **c)** There are training awareness resources available for viewing and download at: www.saic.com/CyberNEXS/#media-downloads, and a pre-recorded video of a CyberNEXS session to demonstrate the functionality that students will use during the Finals, at: www.saic.com/CyberNEXS/video.html.
   - **d)** All team members will wear badges identifying team affiliation at all times during the competition.
   - **e)** Each team will designate a Team Captain for the duration of the competition to act as the team liaison between the competition staff and their team before and during the competition.
   - **f)** No offensive activity against the competition equipment, the Red Team, or the other teams is allowed. Any activity of this nature will result in the disqualification of the Blue Team conducting it.
   - **g)** The student teams are responsible for
     i) Maintaining the target systems and network defenses

ii) Reviewing initial system configurations to verify that machines are properly configured and patched against vulnerabilities
iii) Managing network and host-based systems to thwart any active threat
iv) Reporting computer misuse to operational staff
v) NOT modifying in any way users named "CNDXAdmin", "CNDXUser", "CNDXAdm", "CyberNEXSAdmin", "CyberNEXSUser", and "CyberNEXSAdm". These accounts are used for administration purposes and are not used to gain red team access to your systems.
vi) Allowing ICMP (ping) within the internal network and to external devices, other than the firewall.
vii) Following the guidelines set forth in your appropriate network security policy for securing your network.

h) Use of automated patching tools (i.e. Up2date, Windows "Automatic Updates" service, etc.) is not allowed except for identified client machines.

i) Network priorities are availability and security. Basically, do what needs to be done to secure the network without denying services to legitimate users.

2) **Competition Systems**

a) Each team will start the competition with identically configured networked systems.

b) Teams may not remove any computer, printer, or networking device from the competition area.

c) Teams should not assume any competition system is properly functioning or secure; they are assuming recently hired administrator positions and are assuming responsibility for each of their systems.

d) All teams will be connected to a central scoring system.

e) Throughout the competition, White Team members will be responsible for maintaining the competition equipment and can troubleshoot systems that malfunction when this malfunction is not part of the competition itself. White Team members are also responsible for judging functions during the competition.

f) Teams must not connect any outside devices or peripherals to the competition network.

g) Teams are not permitted to remove or alter any labels/stickers that are present on their assigned systems.

h) Teams may not modify the hardware configurations of competition systems. Teams must not open the case of any server, printer, PC, monitor, KVM, router, switch, firewall, or any other piece of equipment used during the competition. All hardware related questions and issues should be referred to the White Team.

i) A Red Team will emulate the inside and outside hacker threat that exists on networks today. The type of network activity conducted by the Red Team may include:

1) Enumeration, discovery, and port scanning using RFC-compliant ICMP packets and TCP and UDP connections
2) Attempted logins using guessed and discovered account names and passwords
3) Network sniffing, traffic monitoring, and traffic analysis
4) Use of exploit code for leveraging discovered vulnerabilities

5) Password cracking via capture and scanning of authentication databases
6) Spoofing or deceiving servers regarding network traffic
7) Alteration of running system configuration except where denial of service would result
8) Denial of service attacks, directed, distributed, or otherwise
9) Scanning of user file content
10) Introduction of viruses, worms, Trojan horses, or other malicious code
11) Alteration of system configuration stored on disk
12) Changing passwords or adding user accounts
13) Spoofing or deceiving servers via dynamic routing updates or name service (DNS)

3) Competition Play

a. The competition will be conducted over a nine hour period (one hour for lunch).
b. Operating Systems: Windows
Other devices: Firewalls, Intrusion Detection System (IDS), Switches and Routers, Network Management System and a Trouble Ticketing System.
c. The number of "Blue" Targets: Seven (see Blue Team Systems section below)
d. The competition will be conducted for eight hours (8AM-11AM; (1) Hour Lunch Break; 12PM-5PM EST); the competition play will freeze for one hour during lunch.
e. During the competition team members are forbidden from entering or attempting to enter another team's competition workspace.
f. Teams must compete without "outside assistance" from non-team members which includes team advisors and sponsors. All private communications (calls, emails, chat, directed emails, forum postings, conversations, requests for assistance, etc) with non-team members, including team sponsors that would help the team gain an unfair advantage, are not allowed and are grounds for disqualification.
g. No PDAs, memory sticks, CDROMs, electronic media, or other similar electronic devices are allowed in the room during the competition unless specifically authorized by the White Team in advance. All cellular calls must be made and received outside of competition area. Any violation of these rules will result in disqualification of the team member and a penalty assigned to the member's team.
h. Teams may not bring any computer, tablets, PDA, or other wireless device into the competition area. Laptop computers (Windows XP), intrusion detection systems (Snort) and an on-line library of software resources will be provided for the student's use.
i. Printed reference materials (books, magazines, checklists) are permitted in competition areas and teams may bring printed reference materials to the competition.
j. Team sponsors and observers are not competitors and are prohibited from directly assisting any competitor through direct advice, "suggestions", or hands-on assistance. Any team sponsor or observers found assisting a team will be asked to leave the competition area for the duration of the competition and a penalty will be assessed against the team.
k. Team members will not initiate any contact with members of the Red Team during the hours of live competition. Team members are free to talk to Red Team members, White Team members, other competitors, etc. outside of competition hours.
l. On occasion, White Team members may escort individuals (VIPs, press, etc) through the competition area.

m. Only White Team members will be allowed in competition areas outside of competition hours.
n. Teams are free to examine their own systems but no offensive activity against the White Team, other teams, or the Red Team will be tolerated. This includes port scans, unauthorized connection attempts, vulnerability scans, etc. Any team performing offensive activity against other teams, the White Team or the Red Team will be immediately disqualified from the competition. If there are any questions or concerns during the competition about whether or not specific actions can be considered offensive in nature contact the White Team before performing those actions.
o. Teams that are the most successful are those who proactively collaborate with their teammates.

4) Scoring

a) There will be one champion declared at the completion of the competition; the 2010 Mayor's Cyber Cup Champion will be the team with the highest overall score.
b) Scores will be monitored by the White Team, but will not be shared until the end of the competition day.
c) Any team that tampers with or interferes with the scoring system (ScoreBot) or with another team will be disqualified.
d) Students will be evaluated in four skill areas:

5) maintenance of critical services;
6) removing vulnerabilities and hardening systems;
7) communicating status and resource requirements; and,
8) thwarting attacks.

5) Questions and Disputes

a. Team captains are encouraged to work with the competition officials to resolve any questions or disputes regarding the rules of the competition or scoring methods before the competition begins.
b. Protests by any team will be presented by the Team Captain to the competition officials as soon as possible. The competition officials will be the final arbitrators for any protests or questions arising before, during, or after the competition and rulings by the competition officials are final.
c. In the event of an individual disqualification, that team member must leave the competition area immediately and must not re-enter the competition area at any time. Disqualified individuals are ineligible for any awards.
d. In the event of a team disqualification, the entire team must leave the competition area immediately and is ineligible for any individual or team award. If competing virtually, that team's game will be stopped and the connection dropped.

6) System Requirements for Centralized Game Contestants

<u>Hardware Requirements are as follows</u>:

A. Windows/Macintosh/Linux computer that is supported by the SSL VPN server

B. 1 Ghz or higher processor;
C. 1 GB RAM minimum;
D. Keyboard & Mouse;
E. 1024x768 or higher display; and,
F. Network connection from computer(s) to Internet. (As specified below)

Software Requirements are as follows:

A. Web Browser (JavaScript capable)
B. SSH Client;
C. VPN Client;
D. Telnet;
E. RDC (Remote Desktop Connection); and,
F. VNC (Virtual Network Computing).

Network Requirements are as follows:

A. Each user needs a network connection with a minimum of 256Kbps internet connectivity (uplink and downlink) and under 150 ms response time to SAIC VPN
B. Network firewalls and/or Web Proxies should permit out-bound SSL VPN connections to cybernexs-vpn.saic.com.

Scoring Described

The winner will be based on the highest overall team score at the end of the competition. The scores are based on the following metrics:

Defense Criteria

- Successful Attack on Blue deducts 10 percentage points
- Success in maintaining critical services adds percentage points
- Success in removing vulnerabilities adds percentage points

Trouble Ticket Criteria

- Quality and timeliness of Trouble Tickets. Scoring noted below
  - +0.5% - Notices a problem, but doesn't have much detail
  - +2.5% - Notices a problem, shows IDS or system logs confirming problem
  - +5.0% - Identifies problem, and details description of fix.
  - +7.5% - Fixes problem, and details system re-configuration
  - +10.0% - Detects Attacker, Identifies & Fixes Problem, provides complete details

Other Items

1) Questions

For Practice and Qualification Rounds, there will be no real-time technical support available due to the large number of competing teams. There will be on-line tools available to validate system configuration and connectivity that can be used during the Practice Round to verify. Nevertheless, competitors should notify their local IT Department as soon any difficulty accessing the system is detected.

During the Finals, the White Team will assist with any questions concerning game play.

2) Preparations

There are on-line training materials available at the following websites:

SAIC's CyberNEXS Security Tips Videos: http://www.saic.com/CyberNEXS/#media-downloads

AFA/UTSA Web site: http://www.highschoolcdc.com

Description of CyberNEXS

CyberNEXS Overview

In today's increasing hostile communications environment, a strong computer network defense (CND) program is the key to an organization maintaining maximum availability and security of their data networks. To most effectively prepare an IT organization, the "Security Team" needs to routinely train as they would operate in their everyday environment. They need to not only rehearse against realistic attack scenarios but they must also train on IT systems that mirror their own infrastructure. Finally, training as a Team is critical to ensure that they can administer and coordinate the many functions of computer network defense, which include: secure system configuration, intrusion detection, incident analysis, forensics, misuse data collection and incident mitigation. In response to this need, SAIC developed the Cyber Network EXercise System (CyberNEXS), which assists the organization's Chief Information Office (CIO) in the training and evaluation of their CND team's ability to detect network attacks/intrusions and defend their critical information resources from those attacks. It provides near-real time feedback in a realistic environment where new network defense tactics, techniques and procedures (TTP) can be developed, tested and integrated.

The SAIC CyberNEXS system was selected as the competition platform because of its scalability, real world IT systems, and scoring system that produces high-fidelity, credible feedback of contestant's progress. The CyberNEXS service is performed in a controlled training environment, emulating real-world systems and threat activity. The training environment should include representative network, server and workstation systems that the students are expected to configure and maintain in the highest state of readiness. Additionally, an evaluation system has been implemented that will automatically sample system configurations to ensure that the students have installed the most up-to-date vulnerability fixes. It will also determine whether or not a system has been successfully attacked and whether critical services are being interrupted.

The training objectives will therefore evaluate the student's ability to:

a. Maintain critical services while under attack;

b. Identify vulnerabilities and lock down systems (network, server and/or workstation) according to the organization's security policy;

c. Configure router policies according to the organization's security policy (University only);

d. Configure and monitor network-based and host-based intrusion detection systems (NIDS/HIDS) (University only); and,

e. Recognize and properly respond to hacker/computer misuse activity.

Please visit www.saic.com/cybernexs/video.html for a pre-recorded live demonstration of CyberNEXS.

Profile of Blue System for Practice Round

CYBER_PRACTICE

- Operating System
  - Windows Server 2003 Enterprise
- PURPOSE
  - Custom built with vulnerabilities for Practice Round
- CRITICAL SERVICES
  - CngClient
  - NetBIOS TCP/139
  - TCP/IP NetBIOS helper
  - Terminal Services TCP/3389
  - DNS Client

Profile of Blue System for Qualification Round

CP-EXCHANGE

- Operating System
  - Windows Server 2003 Enterprise
- PURPOSE
  - Custom built with vulnerabilities for Qualification Round
- CRITICAL SERVICES
  - CngClient
  - NetBIOS TCP/139
  - TCP/IP NetBIOS helper
  - Terminal Services TCP/3389
  - DNS Client

Profile of Blue Systems for Finals

W2K3-DC

- Operating System
  - Windows 2000 Server
- Purpose
  - Windows 2003 Domain Controller/DNS Server/DHCP server
- Critical Services
  - DNS (DOMAIN) TCP/53
  - DHCP UDP/67
  - NetBIOS TCP/139
  - SNMP UDP/161
  - Microsoft-DS TCP/445
  - MS-TERMSRV TCP/3389

W2K3-WWW

- Operating System
  - Windows 2000 Server
- Purpose
  - Windows 2003 internal web server
- Critical Services
  - HTTP TCP/80
  - NetBIOS TCP/139
  - SNMP UDP/161
  - HTTPS TCP/443
  - Microsoft-DS TCP/445
  - MS-TERMSRV TCP/3389

W2K-SQL

- Operating System
  - Windows 2000 Server
- Purpose
  - Windows 2000 server/SQL server
- Critical Services
  - NetBIOS TCP/139
  - SNMP UDP/161
  - Microsoft-DS TCP/445
  - MS-SQL TCP/1433
  - MS-TERMSRV TCP/3389

VISTA-WKSTA

- Operating System
  - Windows Vista
- Purpose
  - Windows Vista Workstation
- Critical Services
  - SNMP UDP/161
  - Microsoft-DS TCP/445
  - MS-TERMSRV TCP/3389

XP-WKSTA

- Operating System
  - Windows XP SP2
- Purpose
  - Windows XP with Service Pack 2 workstation
- Critical Services
  - SNMP UDP/161
  - Microsoft-DS TCP/445
  - MS-TERMSRV TCP/3389

PRACTICE ROUND DO's and DON'Ts

Windows 2003 Virtual Machine:

1. DO **Work within the Windows 2003 Virtual Machine image ONLY!**
   Only the changes you make within the virtual machine will be included in your score.

2. DO NOT **delete the Round 1 VM image once the exercise is started and you have registered**
   It contains your unique registration ID and identifies you to the scoring system located at SAIC. If your unique ID is removed, you will have to re-register and your score will return to zero.

3. DO NOT **Disconnect VMWare Devices →Network Adapter**
   While you are working, your virtual machine is constantly communicating to the scoring system located at SAIC. If you are disconnected from the network, your system will be seen as "down" and your score will be inversely affected.

4. DO NOT **Change Devices → Network Adapter → NAT**
   Changing to "Bridged" or "Host-Only" will affect your network connectivity and you will lose connection to the scoring system.

5. DO NOT **RE-LOAD another copy of the Round One Image without re-registering**
   Each VMware Image needs to be individually registered, if you damage your Round One Image to the point, that you feel that the only solution is to start over, then you **MUST** go through all of the registration steps again, choosing a new system name or Team Nickname.

6. DO NOT **Run any Communications Check Images while you are running through the exercise. These images should have been deleted before the Round One image was started.**

   NOTE: You will have to re-do all the changes you made previously, and you will have to work quickly since you have lost valuable time.

Users:

1. **The Administrator account is set to auto-login, if you change this DO remember the password.**
   The initial password (until you change it) is "**admin**" (without the quotes). If you change the password, write it down to ensure you don't forget it.

2. DO NOT **modify, disable, delete, or change the password of CYBERNEXS_ADMIN user**
   This user enables the CngClient service to connect to the scoring system. Tampering with this user may cause your system to stop reporting updates. This includes changing the group.

3. DO **NOT disable or delete Administrator user**
   Since you auto-login with the administrator account, if you disable this account, you won't be able to login. If you choose to disable the auto-login, ***make sure you remember the username and password before you log out***. Otherwise, you may find yourself locked out of the system.

Services:

1. DO NOT **disable, stop, or Modify the CngClient service parameters**
   This is the main service that communicates with the CyberNEXS scoring system at SAIC. If this service is not running, you will not receive a score.

2. **DO NOT disable or stop these services:**
    - **netbios**
    - **TCP/IP NetBIOS Helper (LmHosts)**
    - **Terminal Services (TermService)**
    - **DNS Client (Dnscache)**

    These services have been identified as critical to network connectivity.

    For more details on Windows 2003 services, see http://smallvoid.com/articles/windows-2003/services/

    NOTE: If you follow the smallvoid.com "Trimmed" configuration recommendation, you will disable your own networking and thus will not be able to connect to the internet, and won't be able to score.

Files:

1. **DO NOT uninstall CngClient or delete or modify any files in C:\SAIC\CngClient or**
   The CngClient program runs as a service that constantly evaluates your system health and configuration.

2. **DO NOT delete the C:\Get My Status.html file or the C:\SAIC\CngClient\client.id file**
   These files contain your unique registration id and identify you to the scoring system located at SAIC.

Environment:

1. **DO NOT Delete or modify the CNGCLIENT_CONFIG_HOME environment variable**
   This variable is used within the CngClient program.